App Information Privacy Concerns

Full Paper

Christoph Buck
University of Bayreuth
christoph.buck@uni-bayreuth.de

Simone Burster
University of Bayreuth
simone.burster@uni-bayreuth.de

Abstract

Due to the new technological developments and solutions a new user of information systems evolved. Smart Mobile Devices (SMD) and software in form of mobile applications (apps) diffused into the everyday life of users. The download and usage of apps became ubiquitous and by giving away personal data while using apps, individuals put their privacy at risk. Privacy concerns are generally used to measure information privacy. However, privacy is highly context dependent and needs to be adapted to the investigated environment. Therefore, the authors developed a measurement for app information privacy concerns (AIPC), based on existing literature. A data set of 269 participants was analyzed. For the AIPC three first-order dimensions (anxiety, personal attitude, and requirements) were revealed.

Keywords

Information privacy, privacy concern, personal data, mobile applications, principal axis factoring analysis.

Introduction

Today´s information systems cover and support the most of consumers' everyday life and made Weisers' vision of ubiquitous computing come true (Weiser 1991). Induced by new technological developments and solutions a new user of information systems evolved. Following the notion of experiential computing the user of today´s information systems takes part in "digitally mediated embodied experiences in everyday activities through everyday artefacts with embedded computing capabilities" (Yoo 2010: 213). Starting from supporting applications (e.g., clock, alarm, calendar, calculator, to-do list), connecting applications (e.g., mail, messenger, social media), entertaining applications (e.g., streaming, gaming, sports), up to smart and connected environments (e.g., smart home, smart living) users everyday life is saturated with, mostly invisible, information systems. By the mass adoption of Smart Mobile Devices (SMD) software in form of mobile applications (apps) diffused into the everyday life of users. Thus, apps are integral to the functioning of SMD and are key elements for the interface design and functionality. For many online-based or technology-related value propositions, apps are therefore one of the most commonly used technological interfaces within a smart network of connected devices. Apps can be interpreted as today's archetype example of ubiquitous computing, i.e. the creation of environments saturated with computing and communication capability, integrated with human users (Weiser 1991).

Throughout these functions, the possibilities of gathering personal data are virtually endless. Future prospects in relation to these applications promise even more opportunities to expand data collection and immediate analysis of data. The quality of personal data has substantially improved due to developments in mobile technology and the increasing digitalization of everyday tasks. That leads to continuously updated and integrated personal data generated within mobile ecosystems (Buck et al. 2014). This excessive level of integration does not come without consequences. Individuals' use of apps poses multiple challenges for IS research, especially in privacy research. Personal and personalized user and usage data has huge economic value (Acquisti et al. 2015). Consequently, most apps are traded against privacy because of their valuable data. Nevertheless, research brings to light that individuals are concerned about their privacy and that they are very sensible regarding the collection and use of their personal data (Grossklags and Acquisti 2007).

The recent literature provides multiple constructs and items to measure privacy concerns, but no concern especially for the download and usage of apps. To get a better understanding of individuals' attitude and

behavior it is crucial to examine the contextual nature of privacy. Therefore, the authors of this paper have developed an App Information Privacy Concern (AIPC) to incorporate the contextual factors of apps. The AIPC is developed for further research in information systems research as well as for research in social sciences. Existing scales for privacy concerns where analyzed and used as a foundation for the newly developed AIPC. To evaluate the AIPC the authors conducted a principal axis analysis and provide three new first-order constructs.

This article is structured as follows. In the next section the theoretical foundations regarding information privacy, privacy concerns and the contextual dependency of information privacy are posed. Subsequently, the development of the AIPC is provided. The paper ends with a conclusion and further research.

Theoretical Foundations

Defining Information Privacy

Privacy is called an "umbrella term" because it is addressed in plenty fields of social sciences (Solove 2007). Since different definitions are used in various areas the term lacks a holistic definition (Smith et al. 2011; Solove 2006). First of all, physical and information privacy have to be distinguished. Physical privacy relates to the "access to an individual and/or the individual's surroundings and private space" (Smith et al. 2011: 990). Contrary, information privacy only refers to information that is individually identifiable or describes the private informational spheres of an individual. Although information privacy is rooted in the fundamental concept of physical privacy, both are subsumed under the term of general privacy (Smith et al. 2011).

Even though privacy has developed and changed drastically over the last decades, Westin's definition still holds true: information privacy is defined as "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967: 7). Following Westin, 'control' is construed as an instrument of the protection of privacy, that privacy itself is often defined as the control over personal information (Solove 2006). This control-oriented definition is consistent with earlier definitions of Altman (1975), Margulis (1977). In this paper information privacy is defined as the ability to control the acquisition and use of one's personal information (Westin 1967).

The concept of autonomous and self-determined control over the disclosure of private information is closely related to information and communication technologies and therewith to SMD and apps (Dinev and Hart 2006). Within the scope of IS, such as SMD and apps, personal information is gathered by personal data. Thus, this article treats personal information and personal data as equal. We will keep the following principle throughout the remainder of this article: we will use the term privacy as a reference to information privacy, which is our immediate focus. Regarding data quality, recent developments in mobile technology and an ever-increasing digitization of everyday tasks, lead to an unprecedented precision of continuously updated and integrated personal data, which is generated within mobile ecosystems (Buck et al. 2014). Consequently, apps layer everyday activities and lives in a digital way; or how Clarke rephrased it: "Cyberspace is invading private space" (Clarke 1999: 60). In app markets, individuals are able to control their privacy disclosure during the purchasing process. Thus, individuals can actively control their disclosure of personal data and the grasping of privacy from third parties (Chen and Chen 2015). In conclusion, when downloading and using apps consumers put their privacy at risk on a very high level.

Current Measurements of Information Privacy Concerns

As monitoring of personal information is ubiquitous the concerns about information privacy are growing and it has been a major research field since the mid-1990s (Dinev et al. 2015). It is almost impossible to measure privacy itself as it depends more on cognitions and perceptions rather than on rational decision-making. Therefore, almost all empirical privacy studies in social sciences are based on a privacy-related proxy used as a measurement of information privacy (Bélanger and Crossler 2011; Smith et al. 2011; Xu et al. 2012). Privacy concerns have emerged as a fundamental construct in privacy research (Bélanger and Crossler 2011; Li 2011; Smith et al. 2011). There is no universal definition for privacy concerns. However,

in general it refers to the "degree to which an individual perceived a potential for a loss associated with personal information" (Pavlou 2011: 981).

In several studies, different scales have been developed to empirically measure privacy concerns. The groundwork was established by Smith et al. (1996) who developed a multidimensional scale for the Concern For Information Privacy (CFIP). The instrument was rigorously verified and reached a high degree of confidence in scales of validity, reliability and generalizability (Smith et al. 1996). Later, the measurement was revalidated by Stewart and Segars (2002) and empirically confirmed. Consequently, the CFIP was applied in various empirical studies and plays a significant role in the privacy macro-models of Smith et al. (2011), Bélanger and Crossler (2011) and Li (2011). Besides, it was the foundation of further developments and enhancements of scales to measure information privacy concerns. Malhotra et al. (2004) used the CFIP as a groundwork and adapted it to the context of the Internet. They established a framework on the dimensionality of Internet Users' Information Privacy Concerns (IUIPC). It is conceptualized as "the degree to which an Internet user is concerned about online marketers' collection of personal information, the user's control over the collected information, and the user's awareness of how the collected information is used" (Malhotra et al. 2004: 338). It is a useful tool to examine the reactions of online consumers in the context of various threats on the Internet (Malhotra et al. 2004). Further enhancements of the CFIP applied to the context of mobile systems was developed by Xu et al. (2012). The scale to measure Mobile Users' Information Privacy Concerns (MUIPC) is subdivided into three first-order dimensions. An overview of the previously discussed scales to measure information privacy is given in table 1.

	CFIP (15-item scale)	IUICP (10-item scale)	MUICP (9-item scale)
Purpose	To reflect individuals' concern about organizational privacy practices.	To reflect Internet users' concerns about information privacy.	To reflect mobile users' concerns about information privacy.
Focus	Organizations' responsibilities for the proper handling of customer information.	Individuals' subjective views of fairness within the context of information privacy.	Individuals' feelings that one has the right to own private information
First-order Dimensions	•Collection •Unauthorized secondary use •Error •Improper Access	•Collection •Control •Awareness of privacy practices	•Perceived surveillance •Perceived intrusion •Secondary use of information

Table 1. Overview of Privacy Concern Measurements (adapted from Xu et al. 2012)

Despite the different scales, the CFIP is used way more frequently in comparison to the IUIPC (Bélanger and Crossler 2011). As a recommendation for information privacy research they stated to "create and utilize more validated instruments so that future privacy research can more readily build upon one another" (Bélanger and Crossler 2011: 1035). To be able to get a valid and accurate measurement it is crucial to consider the shifting dimensions and the major influence of the contextual environment. Information privacy concern of mobile users do most likely differ from online consumers which leads to different perceived threats (Malhotra et al. 2004; Xu et al. 2012).

The Contextual Dependence of App Privacy

Information privacy is subject of many research fields not only information systems but also marketing, law, management, psychology and many others. Due to the different research fields it becomes obvious that no matter how information privacy is defined, the issues surrounding the term are myriad and varied (Bélanger and Crossler 2011). Therefore, the individual context is important and shapes the meaning of

information privacy (Nissenbaum 2009; Smith et al. 2011). To improve the understanding of individuals' attitude and behavior it is crucial to examine the contextual nature of privacy. Context has been defined as "stimuli and phenomena that surround and thus exist in the environment external to the individual, most often at a different level of analysis" (Mowday and Sutton 1993: 198). It can be related to many different variables for example, to the discipline of research, time, location, occupation, culture and rationale (Bansal and Zahedi 2008). Privacy is a universal human need and therefore, all individuals can be classified as privacy pragmatist, privacy fundamentalist, or privacy unconcerned depending on time place and situation (Westin 1967; Westin 2003). Depending on the situation and context, individuals can be in a range from extremely concerned about their personal data as far as apathy about privacy (Acquisti et al. 2015). Every purchase decision and the way a product or service is used by an individual is determined by the context in which it takes place (Vargo et al. 2011). This is supported by Spiekermann (2015) who stated that the "context of data exchange is even more important than the data itself" (Spiekermann et al. 2015: 92). In today's mobile environment there is a vast amount of possibilities were data exchange takes place due to the powerful technological surveillance to track and profile individuals.(Xu et al. 2012). Apps are used to perform every kind of task and users benefit while handling their everyday routine which are embedded in mobile ecosystems (Buck et al. 2014). Everyday activities are almost 'naturally' carried out or supported by apps, or as Apple puts it in one of their slogans: "There is an app for that" (Apple Inc. 2017) which captures the broad scope of applications apps are used for. Personal data of individuals is gathered using apps as the majority of them receives, saves or processes personal information. Thus, individuals trade their personal data for the benefit of a "free app" and are often not aware which or even that personal information is used by an app in exchange for the "free" download (Buck et al. 2014). The context is generally associated with how the information is presented. Moreover, it is used as a reference point of individuals to evaluate losses and gains (Goes 2013). In IS environments, such as mobile ecosystems, the context is a complex technological system embedded in a very standardized environment.

The call of Bélanger and Crossler (2011) to create more validated instruments and consider contextual dependence to measure privacy has been adopted by Xu et al. (2012). However, the MUIPC does not reflect all relevant context dependent characteristics of privacy concerns from the literature (e.g. control, collection). Therefore, to provide a picture as complete as possible all measurements of privacy concerns from the literature are taken into account and are then applied to the context of mobile apps. Thus, a new App Information Privacy Concern (AIPC) is developed to measure concerns not only regarding the usage of mobile devices, more so for all smart devices that use apps as a technological interface. Therefore, extant literature regarding the measurement of information privacy concerns have been considered, elaborated, compared and analyzed in detail regarding the contextual factor of mobile ecosystems.

App Information Privacy Concern (AIPC)

Development of the App Information Privacy Concern

To acknowledge for the contextual dependence of privacy we developed a measurement for AIPC established on the existing constructs IUIPC an MUIPC which are based on the CFIP (Malhotra et al. 2004; Smith et al. 1996; Xu et al. 2012). The starting point of the evaluation was the CFIP as it is the groundwork of most subsequent constructs as well as the most frequently used construct in research. CFIP is composed of four first-order dimensions: collection, error, improper access and unauthorized secondary use of personal information (Smith et al. 1996). Comparing those dimensions with the IUIPC and the MUIPC, it becomes noticeable that even if the theoretical foundation differs, collection is also a dimension of the IUIPC (see table 1). Further, unauthorized secondary use of information is integrated in the MUIPC as secondary use of personal information (see table 1). Due to the importance in literature and the good fit to the app context these two dimensions (collection and secondary use of data) are considered for the development of the re-arranged construct. The items of the dimensions error and improper access are evaluated as irrelevant for the app context.

After analyzing the groundwork of the scale and reducing the irrelevant dimensions, in the first step (see figure 1) the IUIPC of Malhotra et al. (2004) is defined as the basis for the new arranged construct. The three first-order dimensions collection, control and awareness of the IUIPC are based on social contract theory (Friend 2004). Those dimensions represent the basis of the AIPC and are enhanced and

supplemented by the MUICP in the second step (see figure 1) which is based on communication privacy management theory (Petronio 2012).

Collection, is defined as "the degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received" (Malhotra et al. 2004: 338). This dimension is adopted from Smith et al. (1996) who stated that individuals often have the perception that great amounts of data regarding their personalities are gathered and they dislike it. Due to the developments in technological capabilities for surveillance, companies are able to collect unreasonable amounts of data (Bellman et al. 2004). This is especially true for the rapid advancements in mobile technologies with aggressive data collection and the impression that users' behavior is constantly monitored through SMD (Xu et al. 2012). According to Solove (2006) surveillance can be defined as "the watching, listening to, or recording of an individual's activities" (Solove 2006: 490). This definition ties in with understanding for collection of data. Xu et al. (2012) adopted this understanding and developed a dimension called perceived surveillance for the MUIPC. This dimension can be perfectly integrated in the collection dimension because surveillance can be seen as passive way of collection. Consequently, the two dimensions are merged and redundant items are deleted (see figure 1).

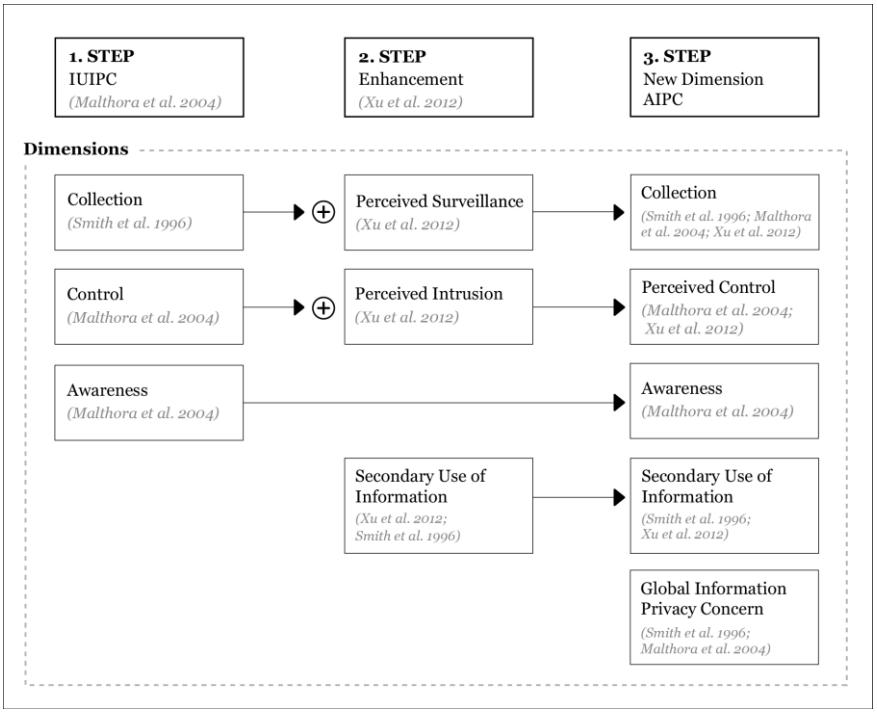

Figure 1. Development of the AIPC

Control, the second dimension of the IUIPC, is an important dimension in the privacy context (Malhotra et al. 2004). This is due to the fact, that the overall definition of information privacy lies on control and the fact that individuals have an interest in controlling or at least in significantly influencing the use of their personal data (Clarke 1999). Malhotra et al. (2004) proposed that "an individual's concerns for information privacy center on whether the individual has control over personal information as manifested by the existence of voice or exit" (Malhotra et al. 2004: 339). This dimension is amplified by the related dimension of perceived intrusion of the MUIPC (Xu et al. 2012). The notion of intrusion has often been related to the concept of personal space which has, due to the development of technology, expanded to physical and informational space (Solove 2006). Solove (2006) defines intrusion as "invasive acts that disturb one's tranquility or solitude" (Solove 2006: 491). Intrusion creates discomfort and harm and therefore individuals have to restore their comfort zones. Therefore, intrusion into the personal space of an individual is related to loss of control. Consequently in the second step, the dimension perceived intrusion is implemented in the dimension control of the IUIPC. Xu et al. (2012) states that individual's perception of intrusion would be triggered "when data recipients are able to make independent decisions

about their personal information" (Xu et al. 2012: 5). This emphasizes that the items of perceived intrusion are closely related to perceived loss of control. Thus, to reflect both dimensions in the third step it is defined as perceived control in the AIPC (see figure 1).

In contrast to control, awareness is a passive dimension of information privacy and defined as "the degree to which a consumer is concerned about his/her awareness of organizational information privacy practices" (Malhotra et al. 2004: 339). This can be perfectly transferred to the context of mobile ecosystems as the app providers' privacy practices are often non-transparent. Individuals are more likely to refuse to reveal personal information if they are not sure how the data will be used. Moreover, individuals are interested in transparency and want more information about how the personal data is used (Malhotra et al. 2004). It is argued that awareness is an important factor for privacy concerns and therefore included in the newly developed construct (see figure 1).

One important dimension which is absent in the IUIPC is unauthorized or secondary use of information (Smith et al. 1996; Xu et al. 2012). According to Smith et al. (1996), it is defined by the concern of individuals that personal information is collected for one particular purpose but used for another without having authorization from this individual to do so. Individuals' attention is drawn, as soon they perceive that their personal data is used for a different purpose or disclosed even to third party who they did not give permission to (Smith et al. 1996). Generally, individuals then feel that their privacy has been violated. Therefore, it is important to include unauthorized or secondary use of information when considering privacy concerns. As the construct of secondary use of information of Xu et al. (2012) (which are adopted from Smith et al. 1996) is adapted to the mobile app context, those items will be used for the AIPC to avoid redundancy (see figure 1). The one dimension that is missing is the general information privacy concern (GIPC) (Smith et al. 1996) which has been adopted by Malhotra et al. (2004) with the aim of capturing overall or general privacy concerns of individuals. This dimension is represented by items like "I am concerned about threats to my personal privacy today" (Malhotra et al. 2004: 352). The GIPC dimension is also added to the newly developed construct. By adding a general concern, it is easier to set other, more specific, constructs in relation and determine if individuals have general privacy concerns (see figure 1). After analyzing the constructs, the underlying items, and the existing overlaps in terms of applicability to apps and mobile ecosystems, we identified 17 items for further investigation and restatement. The AIPC consists of the items shown in table 2.

Abbreviation	Item wording
MaPeCo1	Mobile app privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
MaPeCo2	(Mobile app user) control of personal information lies at the heart of mobile app users' privacy.
XuPeIn2	I believe that as a result of my using mobile apps, information about me that I consider private is now more readily available to others than I would want.
XuPeIn3	I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.
MaAw1	Mobile app providers seeking information online should disclose the way the data are collected, processed, and used.
MaAw2	A good privacy policy for mobile app users should have a clear and conspicuous disclosure.
MaAw3	It is very important to me that I am aware and knowledgeable about how my personal information will be used.
MaColl1	It usually bothers me when mobile apps ask me for personal information.
MaColl2	When mobile apps ask me for personal information, I sometimes think twice before providing it.

XuPeSu2	I am concerned that mobile apps may monitor my activities on my mobile device.
XuPeSu3	I am concerned that mobile apps are collecting too much information about me.
XuSeUPI1	I am concerned that mobile apps may use my personal information for other purposes without notifying me or getting my authorization.
XuSeUPI2	When I give personal information to use mobile apps, I am concerned that apps may use my information for other purposes.
XuSeUPI3	I am concerned that mobile apps may share my personal information with other entities without getting my authorization.
MaGIPC2	Compared to others, I am more sensitive about the way mobile app providers handle my personal information.
MaGIPC3	To me, it is the most important thing to keep my privacy intact from app providers.
MaGIPC6	I am concerned about threats to my personal privacy today.

Table 2. Items of the AIPC

Explorative Factor Analysis

There are several different methods to uncover factors in data sets (Field 2013). The focus of the analysis in this paper is to estimate the construct validity of the newly developed items without generated hypotheses. Therefore, an explorative factor analysis (EFA) is used to test if the items load on factors that measure the individual items. To extract the latent variables a principal axis factoring analysis (PFA) was used to test the 17-items construct on validity.

To evaluate the new construct by PFA, we conducted an online survey were all items of the AIPC were measured by a 7-point Likert-scale ranging from “totally disagree” (1) to “agree completely” (7). A “no opinion” option was available so that responses were not forced. (Bellman et al. 2004). Data collection took place in last week of October until the second week in November 2016 in Germany. 355 participants (n=355) participated in the survey. After deleting incomplete data sets, 269 participants (n=269) were included in the subsequent data analysis. The age of participants ranges from 13 to 66 years (MV=21.57; SD=8.49). Of the remaining participants, 52.8% (n=142) were female and 47.2% were male (n=127).

Running the analysis, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy has a value of p=0.920 which is above the critical value of 0.5 and in the marvellous section according to Hutcheson and Sofroniou (1999). Therefore, we can be confident that the sample size is adequate for factor analysis. Barlett’s Test (p=0.000) is highly significant at a 1% significant level, providing that our sample is suitable for factor analysis.

For the factor extraction we conducted a PFA with oblique rotation (Promax) to discriminate between factors (Field 2013: p.?). To further improve the interpretation of the results, we chose to suppress values below 0.3. “However, the significance of a loading gives little indication of the substantive importance of a variable to a factor” (Field 2013). Nonetheless, Field (2013) does suggest to interpret factor loadings with an absolute value greater than 0.4. An initial analysis was run to obtain eigenvalues for each factor in the data set. We applied Kaiser-Guttmann rule and extracted three factors out of initial 17-item construct with an eigenvalue greater than 1. The three factors explain 60.64% of overall variance. To analyze the results, we examined the pattern matrix to be able to assign the items according to related factors. All items, beside one item (MaColl1), had factor loadings with an absolute value greater than 0.4. However, this value is a guidance and we decided, due to completeness, to include all items to the AIPC construct. The results of the PFA – the three extracted factors and its items - are presented in table 3.

As shown in Table 2 all items loaded cleanly on their respective constructs. There were only cross loadings with considerable high loadings on two factors (item XuSeUPI2 and MaGIPC6). However, the items have with regard to the content a superior fit with factor 1.

Items	Factor 1	Factor 2	Factor 3	Cronbach's alpha - if item deleted
XuPeSu3	**0,861**	0,039	-0,035	0,911
XuPeIn2	**0,783**	-,0289	0,228	0,916
XuPeSu2	**0,749**	-0,037	0,061	0,914
XuPeIn3	**0,740**	-0,098	0,128	0,914
XuSeUPI1	**0,684**	0,210	-0,032	0,912
XuSeUPI3	**0,669**	0,227	-0,100	0,913
XuSeUPI2	**0,580**	0,302	-0,075	0,912
MaGIPC6	**0,507**	0,319	-0,125	0,915
MaAw3	-0,151	**0,834**	0,153	0,915
MaColl2	-0,020	**0,632**	0,137	0,916
MaGIPC3	0,123	**0,618**	-0,029	0,916
MaGIPC2	0,134	**0,517**	0,065	0,917
MaAw2	-0,051	-0,004	**0,772**	0,919
MaAw1	0,014	0,127	**0,700**	0,917
MaPeCo2	0,208	0,046	**0,429**	0,918
MaPeCo1	0,092	0,210	**0,425**	0,917
MaColl1	0,072	0,126	0,253	0,923

Table 3. Results of Principal axis Analysis using Promax Rotation

To measure the reliability of the construct we analyzed all items according to Cronbach's alpha. The overall reliability of the scale is very high with Cronbach's alpha of 0.920 (Field 2013). All items show a high item to item correlation (above 0.3) beside one item. The same is true of the values in the column "Cronbach's alpha if item deleted" of table 2. The same item that scored below 0.4 (MaColl1) in the rotation pattern matrix would also increase the Cronbach's alpha to 0.923 if the item was deleted. However, due to completeness we do not delete the single item.

The three extracted factors are described with "anxiety" (factor 1) which is related to collection, access to and secondary use of personal data and surveillance of activities. The second factor represents "personal attitude" (factor 2) which is related to how important it is for individuals to be informed and their attitude towards disclosure of personal information. The last factor represents "requirements" (factor 3) which is related to requests individuals have towards third parties regarding the handling of their data.

"Anxiety" includes the items XuPeSu3, XuPeIn2, XuPeSu2, XuPeIn3, XuSeUPI1, XuSeUPI3, XuSeUPI2, and MaGIPC6. The dimension is be defined as degree to which a person is concerned about the usage and processing of the collected personal data via mobile apps. The second factor defined as "personal attitude" consists of the four items MaAw3, MaColl2, MaGIPC3, and MaGIPC2. This dimension specifies how important it is for a person to protect their personal data and how sensitive they handle it. "Requirements" as the third factor consists of the items MaAw2, MaAw1, MaPeCo2, MaPeCo1, and MaColl1. This factor can be defined as the degree to which an individuals has request towards third parties regarding the handling of their personal data.

Conclusion and Further Research

Since it is almost impossible to measure privacy itself, social sciences generated privacy concerns as an underlying privacy-related proxy. Because privacy and in particular privacy concerns are highly

contextual dependent this paper presents the measurement for information privacy concerns in the context of apps and mobile ecosystems. The developed AIPC was analyzed by a data set of 269 participants. The first-order dimensions anxiety, personal attitude, and requirements were revealed. The AIPC defines to which degree individuals are concerned about their information privacy regarding mobile apps. In particular it states the anxiety, personal attitude and requirements individuals have regarding the collection, usage and processing of the data gained by mobile apps.

The developed AIPC enables researchers to investigate the field of information privacy concerns with context specific items. Therewith, this paper is in line with the call for research of Dinev et al. (2015), who invite the research community to intensify the endeavors in information privacy because of its upcoming societal and ubiquitous relevance. Nevertheless, the application of the AIPC should be under review dependent on the specific contexts the research takes place. Dependent on the context of further studies this can for example lead to biases like socially desirable response patterns or premature breakup. It is open to discussion whether it would be an improvement for the construct to leave out item MaColl1. From a statistically point this would be the case, however we consider the item as quite important because it measures an important point with its definition "It usually bothers me when mobile apps ask me for personal information." Nonetheless, it underpins the understanding of some individuals that they are not concerned, or to be more precise, to not value their personal information.

Nevertheless, this paper afflicted with some limitations. Firstly, the sample size does not represent all age groups because of the focus on students. Moreover, we did not consider culture bound issues as the sample only consists of German users of SMD (Krasnova and Veltri 2010). In addition, it can be scrutinized if the observed constructs, e.g. the privacy concern, are suitable measures. Therefore, one limitation lies in the multi-item constructs which might be too long and thus participants drift more towards a high-effort process which is not intended when low-effort processing should be measured. Furthermore, a limitation of the study is that the level of participants' literacy (specific knowledge in the field) is not known, e.g. regarding the functionality of apps and the processing of personal information. It is possible that with more elucidation and knowledge transfer in the area of digital ecosystems, individuals are more conscious and reflecting when they are disclosing personal information.

Consequently, we suggest further investigations in this area. To improve the validity of the construct and to confirm the factor structure, future research aims to conduct a confirmatory factor analysis (CFA) to affirm the results obtained from the EFA. Besides, it would be interesting for further research to conduct a cluster analysis in order to profile different user groups.

REFERENCES

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science (New York, N.Y.)* (347:6221), pp. 509–514.

Altman, I. 1975. *The environment and social behavior*: *Privacy, personal space, territory, crowding*, Monterey Calif.: Brooks/Cole.

Apple Inc. 2017. *Apple Trademark List*. URL: https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html

Bansal, G., and Zahedi, F. 2008. "The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation," *ICIS 2008 Proceedings* .

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the Digital Age: A Review of Infomation Privacy Research in Information Systems," *MIS Quarterly* (35:4), pp. 1017–1041.

Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. 2004. "International differences in information privacy concerns: A global survey of consumers," *Information Society* (20:5), pp. 313–324.

Buck, C., Horbel, C., Germelmann, C. C., and Eymann, T. 2014. "The Unconscious App Consumer: Discovering and Comparing the Information - Seeking Patterns," *Twenty Second European Conference on Information Systems* , pp. 1–14.

Chen, H.-T., and Chen, W. 2015. "Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection," *Cyberpsychology, behavior and social networking* (18:1), pp. 13–19.

Clarke, R. 1999. "Internet privacy concerns confirm the case for intervention," *Communications of the ACM* (42:2), pp. 60–67.

Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Psychology & Marketing* (17:1), pp. 61–80.
Dinev, T., McConnell, A. R., and Smith, H. J. 2015. "Research Commentary: Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box," *Information Systems Research* (26:4), pp. 639–655.
Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., and Strahan, E. J. 1999. "Evaluating the use of exploratory factor analysis in psychological research.," *Psychological methods* (4:3), pp. 272–299.
Field, A. 2013. *Discovering statistics using IBM SPSS statistics*: *And sex and drugs and rock 'n' roll*, Los Angeles, London, New Delhi: Sage.
Friend, C. 2004. "Social contract theory," .
Goes, P. B. 2013. "Editor's ' Comments Information Systems Research and Behavioral Economics," *MIS Quarterly* (37:3).
Grossklags, J., and Acquisti, A. 2007. "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information," Information Security , pp. 7–8.
Hutcheson, G. D., and Sofroniou, N. 1999. The multivariate social scientist: Introductory statistics using generalized linear models., London: Sage.
Krasnova, H., and Veltri, N. F. 2010. "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA," in 43rd Hawaii International Conference on System Sciences (HICSS), 2010 ; Honolulu, Hawaii, 5 - 8 Jan. 2010, R. H. Sprague (ed.), Honolulu, Hawaii, USA. 5/1/2010 - 8/1/2010, Piscataway, NJ: IEEE, pp. 1–10
Li, Y. 2011. "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," Communications of the Association for Information Systems (28), pp. 453–496.
Malhotra, N. K., Kim, S. S., Agarwal, J., Tech, G., and Peachtree, W. 2004. "Internet Users ' The Information the Scale , and a Causal (IUIPC)," *Psychology & Marketing* (15:4), pp. 336–355.
Margulis, S. T. 1977. "Conceptions of Privacy: Current Status and Next Steps," *Journal of Social Issues* (33:3), pp. 5–21.
Mowday, R. T., and Sutton, R. I. 1993. "Organizational behaviour: Linking individuals and groups to organizational context," *Annual Review of Psychology* (44), pp. 195–229.
Pavlou, P. A. 2011. "State of the information privacy literature: Where are we now and where should we go?" *Management information systems : mis quarterly* (35:4), pp. 977–988.
Petronio, S. 2012. *Boundaries of privacy: Dialectics of disclosure:* Suny Press.
Smith, H. J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplonary Review," *MIS Quarterly* (35:4), pp. 989–1016.
Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *Management Information Systems Quarterly* (20:2), pp. p 167-196.
Solove, D. J. 2006. "A taxonomy of privacy," *University of Pennsylvania Law Review* (154:3), pp. 477–560.
Solove, D. J. 2007. "I've got nothing to hide' and other misunderstandings of privacy," *San Diego Law Review* (44), pp. 745–772.
Spiekermann, S., Böhme, R., Acquisti, A., and Hui, K.-L. 2015. "Personal Data Markets," *Electronic Markets* (25), pp. 91–93.
Stewart, K. A., and Segars, A. H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," (13:April 2016), pp. 36–49.
Vargo, S. L., Lusch, R. F., Horbel, C., and Wieland, H. 2011. "Alternative logics for service (s): From hybrid systems to service ecosystems.," *Taking the pulse of economic development. Service trends.* , pp. 123–135.
Weiser, M. 1991. "The computer for the 21st century," *Scientific american* (265:3), pp. 94–104.
Westin, A. F. 1967. "Privacy and freedom," New York: Atheneum.
Westin, A. F. 2003. "Social and Political Dimensions of Privacy," *Journal of Social Issues* (59:2), pp. 431–453.
Xu, H., Gupta, S., Rosson, M., and Carroll, J. 2012. "Measuring Mobile Users' Concerns for Information Privacy," *ICIS 2012 Proceedings* .
Yoo, Y. 2010. "Computing in everyday life: a call for research on experiential computing," MIS Quarterly (34:2), pp. 213–231.